The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351RJB UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO COMPEL

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton, Assistant United States Attorney for said District, and Keith A. Becker, Trial Attorney, hereby files this response to Defendant's Third Motion to Compel.[1]

Despite Michaud's claims to the contrary, the United States has provided substantial discovery about the NIT that was authorized pursuant to a warrant issued in the Eastern District of Virginia. The information provided included, among other things, a copy of the computer instructions sent to Michaud's computer that, when executed, produced the NIT results, the NIT results themselves, the date and time the NIT was executed on Michaud's computer, the Website A page that Michaud was accessing when the NIT was executed, and access to computers and digital devices that were seized from Michaud's home and person.

[1] Although captioned as his "third" motion to compel, this appears to be an oversight as this is only the second motion to compel discovery Michaud has filed.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Although Michaud's expert has been provided with the instructions that were delivered to Michaud's computer and the information that was obtained as a result, he now asks this Court to order the discovery of additional information regarding the use and execution of the NIT. His request should be denied for at least two reasons.

First, Michaud fails to demonstrate that the requested information is material to his defense. His articulated reasons for the request are focused entirely upon speculation about matters irrelevant to any purported suppression issues or defense at trial. Nor has he explained how the information already provided is insufficient to present his defense. His request amounts to little more than a fishing expedition, which Rule 16 does not permit.

Second, even if Michaud could show that the information he seeks is material, that information should not be disclosed because it is protected by a qualified law enforcement privilege. Thus, to the extent the Court believes Michaud may be entitled to the information he seeks (he is not), the government asks the Court to set a hearing at which time the government may present evidence *ex parte* and *in camera* (as is the standard method) that would support its claim of privilege.

I. DISCOVERY REQUESTS AND THE GOVERNMENT'S RESPONSES

As the Court is aware, this case arises from an investigation that used a Network Investigative Technique ("NIT") that identified Michaud as a user of a website operating on the Tor network ("Website A") through which registered users like Michaud regularly accessed illegal child pornography.[2] Using information obtained from the NIT, a search warrant was obtained for Michaud's residence and child pornography evidence was located on Michaud's digital devices, as well as other computer-related information identified by the NIT, including a device with the same Media Access Control ("MAC") address identified via the NIT.

[2] Further detail about the website, investigation and the NIT is contained in the government's response to the defendant's motion to suppress, and attachments thereto. Dkt. 47.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

On September 9, 2015, Michaud made a discovery request seeking information regarding the NIT that identified his IP address while he accessed child pornography on "Website A." Michaud requested "[a] detailed description of the 'additional computer instructions' that are downloaded onto target computers and a copy of the NIT's programming code."

On October 30, 2015, the government responded in writing and provided detailed information regarding the deployment of the NIT and the information it collected. With respect to the request for a detailed description of the computer instructions downloaded by target computers, the government stated exactly what information those instructions directed the defendant's "activating" computer to transmit – i.e., that "[t]he computer instructions downloaded onto a target's computer (hereinafter 'activating' computer) directed the 'activating' computer to transmit . . . to a computer controlled by or known to the government" the computer's IP address, a unique identifier generated by the NIT to distinguish the data from other computers, information about whether the NIT had already been delivered to the computer, and the computer's operating system, "Host Name," active operating system username, and Media Access Control ("MAC") address. With respect to Michaud's request for a detailed description of the means by which those instructions are introduced to target computers, the government explained, "[i]n the normal course of operation, websites send content to a visitor's computer. In accordance with the search warrant authorizing the use of the NIT, when an 'activating' computer requested content from Website A, Website A augmented the requested content with the additional computer instructions associated with the NIT." In response to the defendant's request for a "complete copy of all information and data" that was received by the Government in connection with Mr. Michaud's case by means of the NIT, the government provided a comprehensive "user report" that included information and data about Michaud's actions on Website A while it was under government control, including the web pages he accessed and the image files present on those pages, as well as all of the information collected by the NIT. The government also pinpointed for the defense

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

exactly when the NIT was deployed to Michaud's computer and identified his IP address and the Website A content Michaud was browsing at the time. The user report also makes clear that no information, other than that authorized to be collected by the NIT, was collected as a function of the NIT.

Nonetheless, on November 20, 2015, Michaud filed a motion to compel discovery in which he sought what he described as a copy of "the NIT programming code." Dkt. 54. In that motion, he argued that the information was relevant to his already-filed motion to suppress and a "potential" motion pursuant to *Franks v. Delaware*, which he later filed. *Id*. The government opposed on largely the same grounds it opposes the instant motion. Dkt. 74.

Before the hearing on that first motion, however, in a letter dated December 9, 2015, the government offered, without conceding any obligation to do so, "to make available for review, at an FBI facility, the instructions sent to [Michaud]'s computer and executed that produced the NIT results." During a follow-up conversation, defense counsel confirmed that this offer would obviate the need for that issue to be taken up at the hearing. And the substance of the matter was not discussed at the December 14, 2015, hearing nor addressed in the order compelling discovery that resulted.

Defense counsel subsequently informed the government that review at an FBI facility would not be feasible for his expert and requested that the government modify its proposal to permit his expert to retain a copy of the material referenced in the government's December 9 letter. After an agreement regarding an appropriate protective order, the government agreed to modify the terms of the arrangement as requested. A disc containing the computer instructions referenced in the government's letter was provided to the defense expert pursuant to a protective order on January 11, 2016. The following day, defense counsel contacted the government and made requests for additional information pertaining to the government's use and deployment of the NIT that are the subject of the new motion to compel. In response, the government requested an

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

explanation of the basis for the defense request, but the defense declined to do so and instead filed this motion.

II. LAW AND ARGUMENT

A. Michaud Fails to Demonstrate Materiality

Under Rule 16, a criminal defendant has a right to inspect documents, data, or tangible items within the government's "possession, custody, or control" that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). Evidence is "material" under Rule 16 only if it is helpful to the development of a possible defense. *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). "[I]n the context of Rule 16 'the defendant's defense' means the defendant's response to the Government's case in chief." *United States v. Armstrong*, 517 U.S. 456, 462 (1996).

A defendant must make a "threshold showing of materiality" in order to compel discovery under Rule 16(a)(1)(E). *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir.1995). "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present *facts* which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (emphasis added). "[O]rdering production by the government without any preliminary showing of materiality is inconsistent with Rule 16." *Mandel*, 914 F.2d at 1219. In fact, "[w]ithout a factual showing there is no basis upon which the court may exercise its discretion, and for it to ignore the requirement is to abuse its discretion." *Mandel*, 914 F.2d at 1219. Moreover, Rule 16 "does not authorize a fishing expedition." *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012). But that is exactly the nature of the defense request.

Michaud claims, among other things, that the further information described by his expert regarding the NIT is required (1) "so that [his] computer forensics expert can independently determine the full extent of the information the Government seized from [his] computer when it deployed the NIT," (2) "whether the NIT interfered with or compromised any data or computer functions," (3) "whether the Government's

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

representations about how the NIT works in its warrant applications were complete and accurate;" and (4) so that he can "establish the electronic 'chain of custody' for the data." Dkt. 54 at 1-2; Dkt. 115 at 2. He baldly contends, absent any legal argument or explanation, that the information is relevant to his pending motions to suppress and his defense at trial. This is insufficient to meet his burden of showing materiality for the requested information that he seeks. Accordingly, the court should deny his request.

As described in the NIT affidavit, the NIT was comprised of computer instructions that, when successfully downloaded by a user's computer, were "designed to cause the user's computer to transmit certain information to a computer controlled by or known to the government." Dkt. 47, Ex. 1, p. 25, ¶ 33. Those computer instructions, and the information transmitted by them through execution on Michaud's computer, have been provided to the defendant's expert for analysis. Michaud does not contend that the provided instructions did not, or would not have, produced the provided results. Rather, Michaud speculates about whether analysis of other information related to the NIT's use and execution might have some unspecified bearing on his defense at trial or suppression arguments. But this is exactly the sort of fishing expedition that Rule 16 does not permit. Speculation, without facts, does not a showing of materiality make.

The NIT warrant authorized the collection of specified information using certain computer instructions. The information collected and the instructions that were used to collect it have both been provided to the defense. Despite these and the other disclosures about the NIT and its operation on Michaud's computer, Michaud offers only a series of speculative assertions about what information he might uncover were he granted access to this additional information. Yet he offers no explanation how this information might be relevant or material to his defense nor why the information that has already provided would not suffice. The information requested is not material to his defense.

1. The extent of information seized from Michaud's computer

First, Michaud claims he needs additional information "so that [his] computer forensics expert can independently determine the full extent of the information the

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Government seized from [his] computer when it deployed the NIT." Dkt. 115 at 2. Yet, Michaud has available to him the information collected by the NIT and the computer instructions that generated that information. He therefore has everything he would need to "independently determine" the extent of the information collected by the NIT.

Equally important, nothing in Michaud's motion or the declaration from his expert says otherwise. He does not claim, for example, that the computer instructions would have collected information other than what the government disclosed they did. Nor does he even identify what supposed other information *might* have been collected. Rather, Michaud's expert posits, "whether the payload that has been provided was the only payload associated with the NIT or whether other payloads were executed" and claims that he needs to "analyz[e] and understand[] the exploit component of the NIT" in order to determine whether the information provided in discovery "was the only component executing and reporting information to the government" and/or "whether the exploit executed additional functions outside of the scope of the NIT warrant." Tsyrklevich Dec. at 3.

This speculation is wholly irrelevant to the matter at hand. For starters, the NIT results provided to Michaud consist of the only information collected by the NIT. But even if some unspecified additional information were collected by the NIT (or some other set of computer instructions), Michaud does not claim that this unspecified information bears on this case. Nor could he, because the only NIT information relied upon by the government in the warrant for Michaud's home and that it may rely on at trial is that which has already been disclosed.

In short, the government provided information to Michaud regarding what the NIT was authorized to collect, what it collected from his computer, and showed him the computer instructions that did the collecting. His conjecture about some heretofore undisclosed information that could have been collected is irrelevant and immaterial for purposes of Rule 16.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

2. Whether the NIT interfered with or compromised any data or computer functions

Michaud also says that the further information described by his expert regarding the NIT is required to determine "whether the NIT interfered with or compromised any data or computer functions." Dkt. 115 at 2. This too fails to support materiality.

Other than asserting that it is possible, Michaud offers no evidence to suggest that the NIT interfered with or somehow compromised any data or computer functioning. This is telling given that Michaud has available to him tools and information that he might use to support such a theory. Michaud has access to a forensic image copy of his computer and digital devices seized, and this copy is available for examination by a computer forensic expert of his choosing. He has also been provided with substantial information pertaining to his dates of access to Website A, and the date and time at which the NIT identified his IP address accessing the site, and as noted above, he has a copy of the computer instructions that were sent to his computer and generated the NIT results. Despite having that information, he presents nothing to this Court from any examination of that computer or those devices to support his hypothesis that the NIT *could* have interfered with or compromised any data or computer functions, let alone that it did so. Fact, not speculation, is required to support a finding of materiality.

The absence of any factual support for his hypothesis may be explained by the fact Michaud's computer—the one that belonged to him personally as opposed to the one that belonged to the school district that employed him—had software installed on it capable of restoring the computer either to its original factory settings or some other point in time determined by the user of that computer. Significantly, the forensic analysis conducted by the FBI showed that this function was used the night before the FBI executed the warrant at Michaud's home. In any event, the government has made available to Michaud the tools he would need to support his hypothesis. Yet he musters only conjecture. Rule 16 demands more.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

3. Whether the Government's representations about how the NIT works in its warrant applications were complete and accurate

Michaud also says that he needs additional information about the NIT to determine "whether the Government's representations about how the NIT works in its warrant applications were complete and accurate. Dkt. 115 at 2. But again, he does not actually claim that the NIT worked other than as described, just that he needs to verify this is so. Nor, more importantly, does he explain why he cannot achieve this task using the information that has already been provided or what particular aspects of the government's description he cannot test.

In describing how the NIT would operate, the NIT affidavit explained that when a user's computer accessed Website A and downloaded its content in order to display web pages on the user's computer, that content would be augmented with additional computer instructions (which comprised the NIT) that, once downloaded to a user's computer, would cause the user's computer to transmit the information specified in the warrant. Dkt. 47, Ex. 1, p. 24, ¶ 33.[3] And as noted above, those instructions, and the information they generated, have been provided to Michaud. Michaud has also been given substantial information pertaining to the use and execution of the NIT warrant on his computer specifically – including exactly where on the website he was (a posting thread in the pre-teen girls hardcore videos section) when the NIT was deployed to his computer. He also has access to the devices seized from his home. Given all this, the best Michaud can do is hypothesize that the NIT *could* have worked other than as described in the supporting affidavit. He cannot even muster an explanation as to what, if any, aspect of the

[3] Among other details about its execution, the warrant affidavit also explained that variations in the configurations of user's computers might require sending more than one communication in order to get the NIT to activate properly, Dkt. 47, Ex. 1, p. 29, ¶ 44, and that to ensure technical feasibility and avoid detection of the technique by suspects, that the FBI might deploy the NIT discretely against particular users – such as those who had attained a higher status – or in particular areas of the website containing the most egregious examples of child pornography. *Id.*, p. 24, ¶ 32, n. 8. The NIT was deployed to Michaud while he was in one of those areas (Pre-teen Videos – Girls HC).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

description of the NIT contained in the warrant he is unable to test. Surely, Rule 16 requires more.

Michaud's reliance on *United States v. Cedano-Arellano*, 332 F.3d 568 (9th Cir. 2003) (per curiam) to justify his request does not help. In *Cedano-Arellano*, the Ninth Circuit found that the district court abused its discretion when it denied discovery, pursuant to Rule 16, of the certification documents and training materials for the drug dog that had alerted on a defendant's car, where the handler testified about the dog's certification, testing and training at a pre-trial hearing. *Cedano–Arellano*, 332 F.3d at 571. The Court found that the training and certification materials at issue were "crucial to [defendant's] ability to assess the dog's reliability" and "to conduct an effective cross-examination of the dog's handler." *Id.* Here, the NIT consisted of computer instructions, to which Michaud has access, that produced particular results that have also been provided. The NIT results are concrete and verifiable computer information produced through computer instructions that have been provided. [4] Thus, to the extent that *Cedano-Arellano* applies, the instructions already provided are the analogue to the certification and training records.

Significantly, Michaud does not claim that the instructions provided did not or would not generate the NIT information collected by the government. Rather, he merely suggests that reviewing additional information might produce information that might serve as a basis to impeach the NIT warrant. That is vastly different than the situation in *Cedano-Arellano*, and such speculation is not sufficient to trigger a disclosure obligation.

---

[4] The defendant's citation to *Gamez-Orduno* is also unavailing. There, the government failed to disclose a written report of a proffer session with a witness, whom the district court determined to be material because statements during the proffer were inconsistent with factual representations and argument made by the government. The only issue on appeal was the trial court's decision not to dismiss the case. The decision created no broad disclosure obligation for the government but merely acknowledged a seemingly obvious point: withholding evidence, where it has been determined that the evidence is material and helpful to the accused, at a motion to suppress may violate due process if "there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different," and that "[s]uch a due process violation may be cured . . . by belated disclosure of evidence, so long as the disclosure occurs at a time when disclosure would be of value to the accused." *Id.*, 235 F.3d at 461-62 (internal quotations omitted).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Cf. United States v. Guzman-Padilla, 573 F.3d 865, 890 (9th Cir. 2009) ("[M]ere speculation about materials in the government's files [does not require] the district court . . . under *Brady* to make the materials available for [appellant's] inspection.") (citation omitted). Absent the required factual showing, the defendant's request amounts to nothing more than a fishing expedition which is not sanctioned by Rule 16 or any other law.

4. Speculative assertions regarding a digital "chain of custody"

Michaud also says that review of further information about the NIT is necessary to "verify[] the 'chain of custody'" for information derived via the NIT. Dkt. 115 at 2. This request is again purely speculative - he presents no facts whatsoever to suggest that there are or were any issues with the so called "digital 'chain of custody'" pertaining to the NIT-derived information. That the NIT-derived information is computer-related information does not entitle Michaud or his expert to rummage through government's files, digital or otherwise, in the *hope* of finding an error in the chain of custody. *Cf. Guzman-Padilla*, 573 F.3d at 890

None of the cases Michaud cites support his proposition that the government must affirmatively allow analysis of its computers and digital information on the basis of speculation regarding a potential 'chain of custody' issue. In *United States v. McDuffie*, 454 F. App'x 624, 626 (9th Cir. 2011), the Ninth Circuit affirmed the grant of a new trial where the trial court concluded that the late disclosure just prior to trial of the fact that a law enforcement officer's fingerprint was on a drug scale consisted of *Brady* information because it could have impeached the officer's testimony, and he lacked time to retain experts on police procedure or forensics, or engage in pre-trial discovery regarding that piece of trial evidence. 545 Fed. Appx. at 626. In *United States v. Brewster*, the district court denied a defendant's request for a chain of custody document pertaining to a weapon, observing that "[i]t is this Court's experience that when chain of custody is at issue, witnesses simply testify to the issue during trial or at a hearing," in which case, the defendant would "have the right to cross-examine such witnesses" and assuming that

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

pertinent records had been provided. 2009 WL 804709, at *4 (D. Idaho Mar. 27, 2009). Finally, in *United States v. W.R. Grace*, upon a finding that such documents were material, the district court ordered the government to provide chain of custody documentation underlying scientific tests pertaining to asbestos testing. 233 F.R.D. 586, 590 (D. Mont. 2005). None of those cases stand for or support the broad proposition that a defendant may be permitted to rummage through the government's files, digital or otherwise, in search of a speculative chain-of-custody issue, as is proposed here.

5. Other claims of relevance

Michaud's expert also generally claims that additional information pertaining to the use and execution of the NIT is needed to determine "[t]he accuracy and potential admissibility of the evidence collected by the NIT" and speculates regarding whether it is possible that the unique identifier generated by the NIT could be generated incorrectly. Dkt. 115-1 at 3. Michaud's expert has examined the computer instructions sent to Michaud's computer that produced the NIT results, and Michaud has been provided the information transmitted by them. Yet he does not claim that the provided instructions did not, or would not have, produced those results. His questions regarding the accuracy of the NIT data or the theoretical possibility that a unique identifier could have been incorrectly generated rest on conjecture without explanation. Materiality demands fact, not hypothesis. *Cf. Guzman-Padilla*, 573 F.3d at 890.

In addition, there is substantial evidence that bolsters the accuracy of the NIT-derived information. For example, during the search of Michaud's home, FBI seized a network adapter that contains the MAC address reported via the NIT, a thumb drive that was later determined to contain over 2,400 images of child pornography, including images that had been available on Website A, and a 20-page manual entitled "The Jazz Guide: How to Have Sex With Very Young Girls . . . Safely." Dkt. 47, Ex. 4, p. 9, ¶ 31. Michaud's expert takes none of that information into account in making his speculative assertions regarding accuracy of the NIT or the pertinent unique identifier. In light of

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

that information, and his failure to present facts – as opposed to conjecture – to support his assertions, Michaud cannot establish materiality regarding his requests.[5]

B. Information pertaining to the use and execution of the NIT is subject to a qualified law enforcement privilege

Even if the Court believes that disclosure of some or all of the information requested by Michaud is required under Rule 16, a qualified law enforcement privilege applies to bar disclosure because divulging the requested information would be harmful to the public interest. This is so because disclosure could, among other things, diminish the future value of important investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations, and possibly lead to other harmful consequences not suitable for inclusion in this response.[6] As explained below, courts have generally recognized that because of the sensitivity of the information that may support this type of privilege claim, it is appropriate to consider a submission from the government *ex parte* and *in camera*. Accordingly, the United States respectfully requests that the Court permit the United States to offer evidence to support its privilege claim *ex parte* and *in camera*

The privilege has its roots in *United States v. Roviaro*, where the Supreme Court first recognized a qualified "informer's privilege" that protects the identity of government informants. 353 U.S. 53, 59 (1957). Courts have since extended the qualified privilege in *Roviaro* to cover other investigative techniques such as methods of traditional and electronic surveillance. For example, in *United States v. Green*, the D.C. Circuit applied the privilege to bar disclosure of the location of an observation post used in a drug

---

[5] In an attempt to further justify his request, Michaud's expert points to entirely unrelated events that he claims to have occurred in August of 2013, nearly two years prior to the pertinent events in this case, and which appears to be mostly premised upon various news articles speculating about an FBI investigation. Nothing about those events has anything to do with the instant case and, in any event, this sort of speculation-upon-speculation does not furnish any facts to support the materiality of any of Michaud's requests.

[6] The NIT warrant affidavit informed the issuing magistrate that the United States considered the NIT to be covered by law enforcement privilege. Dkt. 47, Ex. 1, p. 30, ¶ 47, n. 9.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

investigation because failing to do so would "likely destroy the future value of that location for police surveillance." 670 F.2d 1148, 1155 (D.C. Cir. 1981). And in *United States v. Van Horn*, the Eleventh Circuit applied the privilege to bar disclosure of the nature and location of electronic surveillance equipment because disclosure would "educate criminals regarding how to protect themselves against police surveillance." 789 F.2d 1492, 1507 (11th Cir. 1986); *see also In re The City of New York*, 607 F.3d 923, 928-29 (2d Cir. 2010) (finding that the district court erred by failing to apply the privilege to reports made by undercover agents because they contained "detailed information about [] undercover operations," disclosure of which would "hinder [law enforcement's] ability to conduct future undercover investigations").

The government bears the initial burden of showing that the law enforcement privilege applies to the materials at issue. *In re The City of New York*, 607 F.3d at 944. Courts then apply a balancing test to determine whether disclosure is required. *Van Horn*, 789 F.2d at 1508. To meet its initial burden, the government must show that the materials contain information that the law enforcement privilege is intended to protect, which includes "information pertaining to law enforcement techniques and procedures, information that would undermine the confidentiality of sources, information that would endanger witness and law enforcement personnel [or] the privacy of individuals involved in an investigation, and information that would otherwise . . . interfere[ ] with an investigation." *City of New York*, 607 F.3d at 944 (citations and internal quotation marks omitted); *see also Commonwealth of Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007) (extending privilege recognized for "confidential government surveillance information" to "law enforcement techniques and procedures.").

Because the evidence required to establish the privilege is often sensitive, court, including the Ninth Circuit, have recognized that it is appropriate to permit the government to make its showing through an *ex parte* and *in camera* evidentiary hearing, the record of which should be sealed for later review. *See, e.g., United States v. Johns*, 948 F.2d 599 (9th Cir. 1991) (over the defense objection, the Court approved district

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

court's consideration of the government's request to maintain the confidentiality of an informant in an *ex parte, in camera* hearing); *United States v. McLaughlin*, 525 F.2d 517, 519 (9th Cir. 1975) (upholding trial court's conduct of *in camera* hearing regarding disclosure of informant's identity and determining that disclosure was not required); *United States v. Alvarez*, 472 F.2d 111, 112-13 (9th Cir. 1973) (same); *United States v. Fixen*, 780 F.2d 1434, 1439-40 (9th Cir. 1986) (suggesting use of *in camera* proceedings to resolve law enforcement privilege issues); *United States v. Kiser*, 716 F.2d 1268, 1273 (9th Cir. 1983) (remanding to district court to conduct *ex parte, in camera* hearing pertaining to *Roviaro* privilege issue and citing cases authorizing in camera hearings in similar situations); *Van Horn*, 789 F.2d at 1508 (district court held *in camera* hearing); *Global Relief Found., Inc. v. O'Neill*, 315 F.3d 748 (7th Cir. 2002) ("Ex parte consideration is common in criminal cases where, say, the identity of information might otherwise be revealed"); *In re Department of Homeland Security*, 459 F.3d 565, 569-71 (5th Cir. 2006) (instructing the district court in a civil case to "review the documents at issue *in camera* to evaluate whether the law enforcement privilege applies"); *City of New York*, 607 F.3d at 949 (determining requesting party did not have compelling need for requested information based upon *in camera* review of the documents); *Rigmaiden*, 844 F.Supp.2d 982 (denying defendant's requests for additional discovery about government investigative technique following *ex parte, in camera* at which the court heard the government's reasons for nondisclosure); *cf. United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998) (while "ex parte hearings are generally disfavored," finding that "[i]n a case involving classified documents, however, *ex parte, in camera* hearings in which government counsel participates to the exclusion of defense counsel are part of the process that the district court may use in order to decide the relevancy of the information.").

At an *ex parte, in camera* hearing, the government can provide a more detailed presentation about both the nature of the information Michaud is requesting and the government's concerns regarding its disclosure. Because of the sensitivity of the

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

additional information requested and for other reasons, simply filing the material under seal with a protective order is inadequate to address the government's concerns. Indeed, courts have recognized that sealing of documents and materials containing such sensitive information is frequently inadequate to prevent its public disclosure. *See, e.g.*, *City of New York*, 607 F.3d 923, 937-39 (citing numerous specific examples of instances where "sealed" materials were inadvertently or intentionally disclosed, and concluding that "[i]n light of how often there are all-too-human lapses with material filed 'under seal'" that it could not "conclude with confidence that filing" the sensitive information would adequately protect the information from public disclosure).

Upon a finding that the privilege applies, there is a "'pretty strong presumption against lifting the privilege.'" *City of New York*, 607 F.3d at 945 (quoting *Dellwood Farms v. Cargill*, 128 F.3d 1122, 1125 (7th Cir. 1997)). The burden shifts to Michaud, who must show that his need for the information overcomes the public interest in non-disclosure. *See Alvarez*, 472 F.2d at 113 (finding, regarding disclosure of informer identity, that "in balancing the interest of the government against that of the accused, the burden of proof is on the defendant to show need for the disclosure."); *see also Van Horn*, 789 F.2d at 1507. The public interest in keeping the information private must be balanced against a defendant's articulated need for the information. *See Roviaro*, 353 U.S. at 628-29. "Whether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the [privileged information], and other relevant factors." *Id.* at 629.

In conducting this balancing, the court should consider the defendant's "need [for] the evidence to conduct his defense and [whether] there are . . . adequate alternative means of getting at the same point. The degree of the handicap [to the defendant] must then be weighed by the trial judge against the policies underlying the privilege." *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982); *see also United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) (the question is "whether the [defendant]

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

demonstrate[s] an authentic 'necessity,' given the circumstances, to overbear the qualified privilege"); *United States v. Foster*, 986 F.2d 541, 543 (D.C. Cir. 1993) (balancing defendant's need for information against importance of government's interest in avoiding disclosure).

In striking this balance, the need for disclosure is more limited in the context of a suppression hearing than at trial. *See McCray v. Illinois*, 386 U.S. 300, 311 (1967); *see also Rigmaiden*, 844 F. Supp. 2d at 990 (applying *McCray* in the context of motion for disclosure of electronic tracking equipment). Even if the party seeking disclosure successfully rebuts the presumption (by a showing of, among other things, a "compelling need"), the court must still then weigh the public interest in non-disclosure against the need of the litigant for access to the privileged information before ultimately deciding whether disclosure is required. *City of New York*, 607 F.3d at 948.

As can be explained in more concrete terms in an *ex parte, in camera* hearing, the public interest in nondisclosure here significantly outweighs defendant's need for the information, particularly in light of the defendant's speculative claims regarding the materiality of the requested information. Disclosure of the requested information would diminish the future value of these investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations, and possibly lead to other harmful consequences not suitable for inclusion in this response. In particular, the risk of circumvention of an investigative technique if information is released has been recognized as a factor in applying law enforcement privilege to electronic surveillance. *See Van Horn*, 789 F.2d at 1508.[7] Accordingly, in the event the Court finds the requested information to be

[7] Risk of circumvention has also been accepted by numerous courts as a basis for non-disclosure, in the civil FOIA context. *See, e.g., James v. U.S. Customs and Border Protection*, 549 F.Supp.2d 1, 10 (D.D.C. 2008) (concluding that CBP properly withheld information under FOIA that "could enable [others] to employ measures to neutralize those techniques"); *Judicial Watch v. U.S. Department of Commerce*, 337 F.Supp.2d 146, 181-82 (D.D.C. 2004)

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

material, the Court should hold an *ex parte, in camera* hearing to assess the applicability of the privilege and the defendant's need for the materials.

The District Court's analysis in *United States v. Rigmaiden* is instructive here. In that case, the government, acting on the authority of a tracking device warrant, used a cellular site simulator in order to locate a wireless "aircard" that assisted in locating and ultimately identifying the defendant.[8] The defendant moved to compel production of additional information pertaining to the technology, methods, and personnel involved in tracking the "aircard." The government provided, as here, substantial information pertaining to the aircard tracking, but opposed disclosure of additional technical details, asserting law enforcement privilege. Following hearings related to the issues, including an *ex parte, in camera* hearing at which the court heard the government's reasons for nondisclosure, the Court denied defendant's requests, finding either they were speculative and accordingly, not material, or that the defendant had not demonstrated a compelling need in light of the government's persuasive showing regarding the law enforcement privilege. *Rigmaiden*, 844 F. Supp. 2d at 996-1004.

Here, Michaud cannot demonstrate any compelling need for the requested information. As demonstrated above, his requests are entirely speculative and conclusory. Those sorts of requests are insufficient to justify a compelling need, in light of the government's assertion of privilege. *See United States v. Buras*, 633 F.2d 1356, 1360 (9th Cir. 1980) (discussing *Roviaro* and holding that defendant's claim that tipster might have exculpatory information insufficient to warrant disclosure); *Guzman-Padilla*, 573 F.3d at 890 (holding that speculation that U.S. Border Patrol policies on use of tire deflation devices might be exculpatory does not justify disclosure under *Brady*). Michaud cannot compel disclosure based simply on his conjecture that the privileged material may contain something relevant.

("even commonly known procedures may be protected from disclosure if the disclosure could reduce or nullify their effectiveness").

[8] An "aircard" may be attached to a laptop computer in order to provide Internet service.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

In addition, Michaud has been provided or has access through discovery to "adequate alternative means of getting at the same point" to which he claims disclosure of the information is relevant. *Harley*, 682 F.2d at 1020. For instance, he has been provided with the computer instructions sent to Michaud's computer and executed that produced the NIT results, and the NIT results – allowing him to verify that the particular instructions would have produced the particular results and therefore that the NIT was properly described in the pertinent warrants. He also has ongoing access to a forensic image copy of his computers and digital devices seized, which he may have examined by a computer forensic expert of his choosing, and substantial information pertaining to his dates of access to the pertinent website, and the date and time at which the NIT identified his IP address accessing the site. He may analyze that information if he wishes to verify that the NIT did not interfere with or compromise any data or computer functions. And to the extent that Michaud wishes to request chain of custody documentation from the government regarding items to be admitted at trial, there are numerous avenues available for Michaud to request such information short of seeking to rummage through the government's files or to compel the government to disclose privileged material. Accordingly, Michaud cannot establish the sort of compelling need required to outweigh the significant public interest in nondisclosure of additional details pertaining to the use and execution of the court-authorized NIT.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

III. CONCLUSION

For all the foregoing reasons, the Court should deny Defendant's motion to compel.

Dated this 21st day of January, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
Matthew P. Hampton
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: (253) 428-3800
Fax: (253) 428-3826
E-mail: matthew.hampton@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on January 21, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney of record for the defendant.

/s/ Matthew P. Hampton
Matthew P. Hampton
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: (253) 428-3800
Fax: (253) 428-3826
E-mail:
matthew.hampton@usdoj.gov